July 31, 1996

Proposed Scrambling/Encryption System for DVD

1. **Coverage**

- The system is designed to be usable in all types of DVD products, including DVD stand-alone players, ROM drives (computer connected players), RAM/R devices (recordable drives)

- The current proposal involves encryption applied to prerecorded media and internal computer communications of material originating on prerecorded media

2. **Basic outline**

- Sequence: (1) audio/video data are compressed and then scrambled to create prerecorded disk; (2) upon playback in a DVD device, the data are descrambled and then decompressed. This approach preserves the normal processing presently used for master preparation for studio operations.

- Upon playback in a DVD device, the data are descrambled, followed by audio-video decompression, with both functions accomplished within the device for stand-alone players. Within a computer, these functions could (and probably would) be accomplished in through separate functional devices or appropriate software.

- Descrambling and decompression accomplished through the use of software would be subject to some kind of "tamper resistant" requirement for the software. An security-based requirement equivalent to "tamper resistance" would need to be devised to apply to hardware applications.

- Copy controls are not specifically addressed by this proposal, but it is assumed that such controls would be present, either as associated data (as in the original CGMS proposal) or embedded data.

3. **Encryption Keys**

- Three keys are used for each prerecorded work: a disc key, a title key, and a control key. The control key is utilized only in the computer environment, as a part

of the internal authentication process during transmission of the other keys to the descrambler and associated decoder.

- All keys are composed of less than 40 bits, making them not subject to export control regimes (other than a limited number of highly sensitive countries).

4. Encryption/decryption process

- For each work that a copyright owner wishes to subject to this system, encryption would proceed as follows:

(1) the content would be scrambled using the Title Key, the algorithms and related system technology. The content owner would determine the Title Key on its own.

(2) the Title Key would be encrypted using the Disc Key (obtained from a key distribution entity, probably a separate part of the independent licensing body described below). The encrypted Title Key would be recorded in the Sector Header area, which is a "hidden" area. ("Hidden" here and elsewhere in this paper means that the area is not readily accessed by the user, except through the special means described below.) This step could either be done by the content owner as part of a master tape or by the disc pressing facility as part of the disc encoding process.

(3) the Disc Key would be converted to "Secured Disc Key Data" -- effectively encrypting this key -- using the Disc Key Protection Hardware Logic. The Secured Disc Key Data would be written in the hidden area of the disc called the "Lead-in Area".

(4) the Control Key is provided on the disc for use in the authentication process applicable to DVD-ROM devices connected in the computer environment. This Key is used to transmit the other keys to the descrambler and associated decoder and is independent of the content scrambling/encryption process itself.

NOTE: The security of the scrambling/encryption process used by studios and disc replication facilities is maintained through both the separate application of keys not necessarily held by the same party and the sealing of the Data Scramble, Title Key Encryption, and Disc Key Protection Logic functions in hardware.

September 17, 1996

DVD Security Management and Licensing Proposal

This memorandum will outline the proposed structure and operations for the DVD Security Management and Licensing Entity (the "Entity"). This Entity should not be confused with the overall DVD consortium, and the following should be read as a proposal.

1. Goals.

The Content Scramble System ("CSS") is designed to provide reasonable security for the contents of DVD disks, thereby alleviating concerns of content providers concerning unauthorized copying of their copyrighted material and facilitating the development of DVD technology. The Entity will be responsible for licensing the technology, supervising the provision of security keys and other critical confidential information, enforcing security restrictions, and handling central administration, all designed to provide security and a level playing field to all participants.

2. Structure.

The Entity will have three main components:

a. Governing Board. The Governing Board will direct and supervise the activities of the Entity. It will include representatives from various affected industries, including the motion picture, computer and consumer electronics industries.

b. Licensing Agent. Companies wishing to adopt CSS will obtain the rights to do so through the Licensing Agent.

c. Security Management Agent. The Security Management Agent ("SMA") will be responsible for administering encryption-related functions in a manner designed to protect the overall CSS system against security breaches.

3. Operations.

a. Scrambling. Disk contents will be scrambled using keys chosen by the content provider or disk replicator. Those keys will be encrypted either through the use of secure hardware provided to content providers or disk replicators or directly by the SMA itself. Disk replicators will then include the encrypted keys in hidden areas on the disk.

b. Descrambling. Licensed DVD players and drives will include special secure hardware which can be used to decrypt the hidden keys on the DVD disk. Manufacturers will obtain that hardware (or the information necessary to manufacture it) from the SMA. When a disk is inserted into a DVD player or drive, the secure hardware will decrypt the hidden keys on that disk. Those keys will then be used to unscramble the contents.

4. Licenses.

In order to participate, content providers, disk replicators and hardware manufacturers will be licensed by the Licensing Agent. Those licenses will include rights to the technology (including necessary intellectual property), and the right to receive necessary information from the SMA. Only licensed disk replicators and/or content providers will have the right to receive secure encryption hardware or encrypted keys from the SMA, and only licensed hardware manufacturers will have the right to include specialized hardware capable of decrypting and reading scrambled contents. Note that these licenses would be required only to encrypt content onto a DVD disk and to decrypt such content. No license would be required from this Entity to manufacture a disk that does not include encrypted contents, or for a player or drive that is only able to read unencrypted content.

License-related fees will be charged only at a level necessary to offset the cost of administration. Restrictions on licensees will be designed to protect the security of the overall system, and to make certain that all participants have a level playing field. Thus, license restrictions may require licensees to provide a license back of their own necessary patents to the Entity and (through the Entity) to other licensees. Licensees would also be required to comply with technical specifications, aimed primarily at preventing the creation of unauthorized copies.

5. Copy Control

Copy control will be accomplished through both technical means inherent in the encryption itself -- e.g., copies of the encrypted version of the contents will not include the keys and will, thus, not be useable by end users -- and through license terms requiring player and drive licensees to implement adequate copy controls within their devices and in the analog and digital outputs of licensed devices.

a. Analog Outputs. NTSC analog outputs of licensed devices will be required to implement either the combination AGC/color stripe Macrovision copy control system agreed upon in March 1996 in the legislative recommendations by CEMA and MPAA or another copy control system shown to be equivalent in terms of both its technical capabilities and its widespread effectiveness on both existing and future analog recorders.

b. Digital Outputs. Digital outputs will be required to have adequate copy control technology as well. The CSS Technology's authentication approach will be defined as meeting this requirement. That approach essentially involves the player or drive "knocking on the door" of the prospective receiving device. If the receiving device has the proper answer, then the "door" can be opened and the content let into that device. Only receiving devices that are themselves licensed will be allowed the information necessary to make the proper response. If other copy control technology becomes available to provide equivalent protection, it will be allowed in place of or in addition to the CSS Technology's authentication approach.

c. Within Licensed Devices. Licensed devices will also be required both to protect the content through refusing to pass keys for encrypted content to unauthorized parts of the devices, through securing pathways along which "in the clear" content may be passed, and through reading and responding to any copy control information contained in or associated with the content (e.g., a recording device would refuse to make a recording of content where copy control information indicates that no copying is allowed). Devices incapable of performing some or all of these functions would either not be licensed or would be prohibited from carrying content to or through portions of devices.

6. Enforcement

Enforcement actions would be available to be taken against licensees that fail to live up to licenses, including specifications and security procedures and against unlicensed uses of the system. Penalties would include revocation of licenses, with other penalties potentially available as well.

Enforcement would be handled through fast-track arbitration, with provision for complaints from licensees as a means of initiating actions. Determinations of whether to take enforcement action and funding for particular enforcement actions would be provided through decisions of the Governing Board or a special enforcement committee of the Board.